KEJAHATAN DUNIA MAYA *(CYBER CRIME)* DALAM SIMAK ONLINE

Antoni*

Abstract: *The development of information technology that occurs today has reached its peak. This can be seen with the rapidly growing features of digital technology, especially internet-based computer technology that resulted in making the "world" getting smaller. Distance and time can be saved with the development of information technology that exists today. All activities that should take a long time and must be traveled a long distance, for now more likely to be accessed anywhere. As with digital technology contained in internet-based computer features, it enables the operation to be completely automated and sophisticated, with computer-readable. As the embodiment of digital technology is the use of online Management Information System (SIMAK) online in teaching and learning activities that are used in education, especially universities. With the use of digital technology in college campus, making academic activities easier. However, various problems on the other hand arise in the application of digital technology used, one of the problems is the possibility of cybercrime such as: manipulation of data that has been incorporated into digital data. Such threats may occur by various malicious parties in the digital world to artificially or alter the digital data already in the entry.*

Kata Kunci: *cyber-crime, SIMAK, Online, information technology*

Seiring dengan semakin berkembangnya tekhnologi yang ada saat ini, mengakibatkan dunia semakin "mengecil" dan "menyempit". Kemajuan tekhnologi yang dimaksud dapat membuat kita semakin mudah untuk mengakses informasi-informasi yang kita butuhkan cukup hanya dengan satu sentuhan jari saja. Perkembangan handphone misalnya, dahulu handphone hanya dapat digunakan untuk berbicara dan mengirim pesan singkat (sms) semata, namun sekarang handphone berkembang layaknya sebuah komputer mini yang canggih. Kecanggihan handphone mengalami perkembangan yang sangat pesat, tadinya menggunakan tekhnologi digital sekarang telah menggunakan tekhnologi layar sentuh dan bahkan kecanggihan tersebut semakin bertambah setelah dipadukan dengan berbagai fitur-fitrur tertentu seperti tekhnologi android dan internet misalnya.

Dengan adanya perpaduan tersebut mengakibatkan tekhnologi handpone berkembang menjadi tekhnologi smartphone (telepon pintar) yang memiliki berbagai macam fungsi termasuk kecanggihan komunikasinya sendiri. Dengan tekhnologi smartphone ini, masyarakat tidak hanya dapat mendengar suara lawan bicaranya saja bahkan sudah dapat bertatap muka secara langsung di handphone tersebut. Selain itu, kecanggihan tekhnologi smartphone juga telah dilengkapi berbagai macam fitur-fitur yang begitu "memanjakan" bagi penggunanya untuk mempermudah merambah di dunia maya (internet). Hal ini dapat penulis contohkan, adanya fitur-fitur yang

*Fakultas Syariah dan Hukum UIN Raden Fatah, alamat koresponden penulis, email: *antoni_uin@radenfatah.ac.id*

memungkinkan seseorang dapat bertransaksi bisnis cukup hanya dengan sentuhan jari tanpa harus bersusah-payah mengantri di bank. Kecanggihan lain misalnya, seseorang dapat membaca dan mengakses berbagai macam berita tanpa harus keluar rumah atau bangun dari tempat tidurnya untuk membeli surat kabar atau menonton televisi. Bahkan saat ini, tekhnologi smartphone juga telah dilengkapi berbagai macam fitur-fitur yang dapat digunakan untuk mengakses berbagai media jejaring sosial (pertemanan), seperti: facebook, twitter, badoo, instagram, flickr, yahoo, dan sebagainya sehingga mempermudah penggunannya untuk berinteraksi dengan masyarakat lainnya, untuk saling bertukar informasi, kabar berita, foto-foto dan bahkan sering juga digunakan untuk berbisnis secara online.

Semua berbagai macam kemajuan yang dimiliki tekhnologi smartphone yang dapat mengakses cepat di dunia maya (internet) ini, secara perlahan namun pasti telah mengubah prilaku baik perorangan maupun masyarakat kita pada umumnya saat ini. Perkembangan tekhnologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial, ekonomi dan budaya masyarakat secara signifikan berlangsung demikian cepat. Selain itu, dengan perkembangan arus informasi dan tekhnologi hari ini menjadi pedang bermata dua, karena selain memberikan kontribusi yang baik/positif bagi masyarakat, juga pada sisi yang lain memberikan dampak-dampak negatif. Dampak negatif dapat timbul ketika terjadi kesalahan yang ditimbulkan oleh piranti komputer yang akan mengakibatkan kerugian besar bagi pengguna atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja tersebut mengarah kepada penyalah gunaan komputer, sehingga berpotensi untuk menggunakan media komputer dan internet untuk melakukan berbagai aksi kejahatan (Andi Hamzah, 1990: 23-24).

Berbagai aksi kejahatan yang menggunakan teknologi komputer dan internet sebagai media-nya, pada akhir-akhir ini menunjukkan angka yang signifikan, baik dari segi kuantitas maupun dari segi kualitasnya. Penggunaan media komputer dan internet sebagai media untuk melakukan aksi kejahatan pada umumnya dikenal dengan istilah *"cryber crime"* (kejahatan dunia maya) (Agus Rahardjo, 2002: 92). *Cyber-crime* juga dapat didefinisikan sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer yang memiliki basis pada kecanggihan teknologi internet (Budi Raharjo, 2002: 23). Sebagaimana yang dikemukakan oleh Andi Hamzah dalam bukunya *"Aspek-aspek Pidana di Bidang Komputer"* (1989) yang mengartikan *cyber-crime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal. Sedangkan menurut Eoghan Casey (2001: 16) *"Cybercrime is used throughout this text to refer to any crime that involves computer and networks, including crimes that do not rely heavily on computer".*

Berbagai macam aksi kejahatan tersebut dimulai dari skala yang ringan hingga yang terberat. Sebagaimana yang dikemukakan oleh Dimitri Mahayana (2015) direktur dari lembaga riset Telematika Sharing Vision yang melakukan penelitian pada 2013, mengatakan Indonesia bisa mendapat 42.000 serangan di dunia maya per hari. Hal ini cenderung dapat merongrong keamanan perusahaan dan negara, serta menghambat perkembangan perseorangan (masyarakat pada umumnya) mengingat mobilitas penggunaan internet yang cenderung meninggat dari hari-kehari.

Tingkat kejahatan dunia maya di Indonesia saat ini mengkhawatirkan, menempatkan Indonesia sebagai urutan satu negara yang paling banyak mendapatkan serangan di dunia maya, menurut data yang muncul dalam acara Indonesia Cyber Crime Summit di Institut Teknologi Bandung (ITB).

Untuk dapat memberikan gambaran lebih lanjut mengenai *cyber-crime* yang pernah terjadi di Indonesia baik yang telah dan sedang diproses oleh pihak Kepolisian Republik Indonesia, dapat penulis kemukakan dalam beberapa contoh kasus berikut ini :

1. Tercatat 64 warga negara Taiwan-Tiongkok yang melancarkan operasi penipuan sibernetika (cybercrime) di Indonesia, akhirnya dideportasi. Pemulangan puluhan pelaku kejahatan lintas negara ini dikawal ketat oleh Kepolisian Daerah Metro Jaya yang dipimpin oleh Direktur Reserse Kriminal Umum Polda Metro Jaya Kombes Krishna Murti. Mereka dipulangkan ke negaranya untuk ditindaklanjuti proses hukumnya (http://www.liputan6.com/tag/penipuan-online, download tgl 7 Nov 2015).;
2. TEMPO.CO, Jakarta - Jumlah kasus kejahatan di dunia maya (*cyber-crime*) di Jakarta yang ditangani Kepolisian Daerah Metro Jakarta Raya meningkat. Sementara pada 2013 jumlah kejahatan yang dilaporkan hanya 541 kasus, pada 2014 tercatat ada 785 laporan. "Tahun ini sampai Agustus 2015 saja sudah 690 kasus," tutur Kepala Bidang Hubungan Masyarakat Polda Metro Jaya Komisaris Besar Muhammad Iqbal, pekan lalu. Kepala Subdirektorat Cyber Crime Polda Metro Jaya Ajun Komisaris Besar Hariyanto mengatakan jumlah korban kejahatan ini paling banyak karena korban mudah percaya akan iming-iming hadiah dan harga murah. "Ini yang membuat kasus penipuan melalui Internet meningkat," ujarnya (https://m.tempo.co/read/news/2015/09/21/064702312/ download tgl 6 Nov 2015) Pukul 20 wib).
3. "Pengaduan tiga bank, yang satu 47 nasabah, satunya sekitar 30 nasabah kemudian ketiga 27 nasabah," kata Deputi Komisioner Pengawasan Perbankan OJK Irwan Lubis kepada Liputan6.com seperti ditulis Kamis (16/4/2015). Irwan menjelaskan, modus pencurian yang dilakukan ialah pelaku atau *hacker* dengan mengunakan virus. Virus tersebut bekerja saat pemiliki rekening bertransaksi menggunakan fasilitas *e-banking* (http://bisnis.liputan6. com/read/2214402/hacker-bobol-ratusan-rekening-nasabah-bank, download tgl 5 Nov 2015)*;*
4. Liputan6.com, Jakarta - Banyak orang pasti pernah mengalami dapat pesan singkat di ponsel dari nomor asing yang mengaku papa, mama, adik ataupun kerabat lainnya dan ujung-ujungnya minta dikirimi pulsa. Modus penipuan semacam ini mulanya tak disadari korbannya, tapi lama kelamaan menjadi rahasia umum dan meresahkan masyarakat. Polisi akhirnya bergerak untuk menghentikan tindak tanduk pelaku. Aparat Subdit Kejahatan dan Kekerasan (Jatanras) Polda Metro Jaya pun meringkus pemimpin salah satu kelompok penipu SMS dengan modus "Mama Minta Pulsa" tersebut di Kota Malili, Sulawesi Selatan, Selasa (3/11/2015) (http://news.liputan6.com /read/2358365/, download Tgl 7 November 2015).

Melihat berbagai kasus yang telah terjadi di dunia maya tersebut di atas telah pada taraf mengkhawatirkan. Sudah seharusnya negara sedini mungkin mengupayakan perlindungan kepada masyarakat luas, mengingat Indonesia sebagai negara yang besar, yang memungkinkan masyarakatnya

sebagian besar adalah pengguna dunia maya (internet) termasuk pemerintah di dalamnya. oleh sebab itu, sebagai salah satu bentuk upaya perlindungan, sudah seharusnya pemerintah sebagai pemegang kebijakan memiliki jarring-jaring pengaman yang "canggih" untuk sesegera mungkin dapat menghentikan atau paling tidak dapat meminimalisir terjadinya atau mencegah kemungkinan timbulnya aksi-aksi kejahatan di dunia maya tersebut. Termasuk di dalamnya adalah membuat berbagai kebijakan-kebijakan yang dapat menjerat pelaku-pelaku kejahatan dunia maya. Selain itu, dimungkinkan untuk dilakukan berbagai sinergisitas dari berbagai pihak untuk bekerja bersama-sama membuat suatu jaringan yang luas tidak hanya di "hilir" namun juga dari "hulunya", untuk menditeksi sejak dini kegiatan-kegiatan yang mengarah kepada penyalah gunaan komputer dengan internetnya. Dengan demikian upaya pencegahan (preventif) dapat dilakukan sejak dini mengingat betapa rumit dan kompleks sistem yang ada pada media internet tersebut.

Jenis-jenis Kejahatan Dunia Maya *(Cyber Crime)*

Sebagaimana telah penulis kemukakan tersebut di atas, dengan semakin berkembannya arus informasi dan tekhnologi terutama internet, menimbulkan dampak positif pada satu sisi juga pada sisi lain menimbulkan dampak negatif. Dampak negatif tersebut cenderung semakin terbuka sehingga dimanfaatkan oleh sebagian orang untuk melakukan berbagai macam penyalah gunaan internet yang cenderung mengarah kepada tindakan kejahatan di dunia maya. Munculnya berbagai kejahatan di dunia maya juga harus diibangi oleh penegakan hukum yang sedimikian rupa (usaha yang rasional) agar dimungkinkan pelaku-pelakunya dapat diproses secara hukum. Untuk memberikan pemahaman kepada kita semua (masyarakat), terutama mengenai kejahatan-kejahatan yang mungkin terjadi di dalam dunia maya, maka dalam kesempatan ini dapat penulis kemukakan sebagai berikut :

1. *Carding* adalah: suatu bentuk penyalah gunaan di dunia maya (cyber-crime) dengan cara berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara illegal (melawan hak), biasanya dengan mencuri data-data dari internet;
2. *Hacking* adalah: kegiatan menerobos program komputer milik orang/pihak lain, dengan maksud-maksud tertentu secara melawan hak. Sedangkan *Hacker* sendiri adalah orang/pelaku yang gemar ngoprek komputer, memiliki keahlian membuat dan membaca program tertentu serta terobsesi mengamati ke amanannya. Hal ini dapat penulis contohkan ada akun media sosial *(face book)* dari teman kita atau akun kita sendiri yang pernah dikuasai secara melawan hak oleh orang-orang yang tidak bertanggung jawab;
3. *Cracking* adalah suatu kegiatan hacking untuk tujuan jahat, sedangkan *"cracker"* adalah "hacker" bertopi hitam *(black hat hacker);*
4. *Defacing* adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang pernah terjadi pada situs Menkoinfo dan Partai Golkar, Bank Indonesia dan Situs KPU saat Pemilu 2004. Tindakan *deface* adalah semata-mata iseng, untuk unjuk kebolehan, pamer kemampuan membuat program namun tak jarang ada juga yang mencuri data-data tertentu untuk kemudian dijual pada pihak lain. Menurut hemat penulis apa-pun

nama nya selagi kegiatan tersebut dilakukan secara melawan hak dan menimbulkan kerugian bagi pihak lain, hal tersebut merupakan tindakan yang melawan hukum;

5. *Phising* adalah: kegiatan memancing pemakai komputer di Internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking, isian data pemakai dan password yang vital;
6. *Spamming* adalah pengiriman berita atau iklan lewat surat elektronik (email) yang tak dikehendakai oleh pemilik email, dengan adanya hal ini terkadang menurut pengalaman penulis sebagai pengguna email terkadang menjadi gangguan tertentu apalagi spamm tersebut begitu banyaknya;
7. *Malware* adalah program komputer yang mencari kelemahan dari suatu software. Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system. Malware terdiri dari berbagai macam yaitu: virus, worm, Trojan horse, adware, browser hijacker dan lain sebagainya.
8. Melihat jenis-jenis kejahatan dalam dunia maya (internet) tersebut, menunjukkan bahwa hampir dalam setiap kegiatan di dunia maya memungkinkan terjadi kejahatan. Oleh sebab itu, sudah seharusnya sebagai pengguna internet yang ke-seharian kita selalu berhubungan dengan internet, harus lebih waspada dan berhati-hati. Kewaspadaan tersebut bukan menjadikan kita harus beralih dan meninggalkan internet, namun sebaliknya kita harus lebih memperdalam pengetahuan kita terhadap fitur-fitur yang ada di internet. Dengan demikian kita dapat memahami kemungkinan "cela-cela" apa yang terdapat dalam internet yang kita manfaatkan tersebut, sehingga memungkinkan pihak ke-tiga yang tidak bertanggung jawab tidak dapat memanfaatkannya sebagai sebagai cela untuk melakukan aktivitas jahat-nya.

Perbedaan *Hacker* dan *Cracker*

Dalam dunia maya (internet) banyak terdapat istilah-istilah tertentu yang hanya dapat dipahami dan dimengerti oleh kalangan internis semata, seperti halnya istilah "hacker dan cracker". Adanya kedua istilah tersebut dalam dunia maya (internet), sering sekali disalah mengerti tentang apa itu hacker dan apa itu cracker. Masyarakat dunia maya berfikir bahwa kedua-nya adalah orang-orang yang selalu melakukan tindakan kejahatan dalam dunia maya. Namun pandangan ini sepenuhnya tidaklah benar, karena di antara hackers tersebut malah ada yang berjasa besar dengan menyelamatkan suatu sistem di internet, sehingga dengan adanya hal tersebut pemilik situs dapat segera memperbaiki situs tersebut. Oleh sebab itu dalam kesempatan ini penulis akan memaparkan apa perbedaan kedua istilah tersebut.

Hacker adalah seseorang atau sekelompok orang yang memberikan sumbangan yang bermanfaat terhadap dunia jaringan internet, sistem operasi, serta memberikan bantuan untuk dunia internet dan computer. Pekerjaan hacker juga dapat dikategorikan sebagai seseorang yang mencari kelemahan dari suatu sistem dan memberikan ide untuk menutup celah atau kelemahan yang terdapat dalam sistem tersebut. apabila melihat hal

tersebut, maka dengan demikian kegitan hacker tersebut ada yang baik dan ada juga hacker yang buruk (yang tidak bertanggung jawab) biasa disebut dengan cracker.

Sebagai mana hacker, pengertian Cracker adalah sebutan untuk seseorang yang mencari kelemahan sistem serta memasukinya guna kepentingan dirinya sendiri (pribadi). Tindakan yang dilakukan oleh *cracker* ini biasanya untuk mencari keuntungan dari sistem yang dimasukinya, seperti halnya sama dengan pencurian data, penggantian atau manipulasi data, penghapusan data serta lain sebagainya. Terdapat juga tool yang digunakan untuk memasuki sistem sebagai alat bantunya.

Modus Operandi Dalam *Cyber Crime*

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi, dapat dikelompokkan dalam beberapa bentuk sesuai dengan modus operandi yang pernah terjadi, maka pada kesempatan ini penulis akan mengemukakan beberapa macam jenis-jenis kejahatan yang sering terjadi di Internet / dunia maya *(cyber-crime)* sebagaimana dikutip dalam Barda Nawawi Arief (2007: 246-247)menurut *Convention on Cyber Crime 2001 di Bunapest Hongaria* yaitu:

1. *Illegal acces/Unauthorized Access to Computer System and Service* (Akses tidak sah ke sistem komputer dan jasa); Adalah suatu bentuk kejahatan yang dilakukan dengan cara merentas atau memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa izin atau tanpa sepengetahuan dari si pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukan kegiatannya dengan maksud sabotase ataupun pencurian informasi yang penting dan bersifat rahasia. Namun dalam prakteknya ada juga kegiatan tersebut dilakukan hanya karena si-pelaku merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi yang tinggi. Modus operandi kejahatan ini semakin meningkat dan berkembang seiring dengan berkembangnya teknologi informasi internet/intranet serta berkembangnya teknologi computer maupun smart phone. Sebagai contoh kasus yang pernah terjadi pada tahun 2000 hacker pernah berhasil menembus masuk ke dalam data base berisi data para pengguna jasa America Online (AOL), sebuah perusahaan milik Amerika Serikat yang bergerak dibidang ecommerce yang memiliki tingkat kerahasian tinggi (Indonesia Observer 26 Juni 2000). Atau pada kasus yang pernah terjadi pada situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para hacker, yang berhasil merentas masuk ke dalam situs milik FBI sehingga mengakibatkan tidak berfungsinya situs tersebut untuk beberapa waktu.
2. *Illegal Contents*

   Merupakan suatu modus *Cyber crime* dengan cara memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh dapat penulis kemukakan pemuatan pemberitaan yang bohong/ tidak benar atau memfitnah yang dampaknya dapat meruntuhkan harkat martabat atau harga diri pihak lain, atau hal-hal yang berhubungan dengan pornografi, pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melakukan

perlawanan pada sebuah pemerintahan yang sah, serta masih banyak lagi contoh-contoh lainnya.

3. *Data Forgery*
   Adalah modus kejahatan dalam dunia maya yang dilakukan dengan cara memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scripless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah pengetikan" yang pada akhirnya akan menguntungkan si-pelaku, karena korban akan memasukkan data pribadi dan nomor kartu kredit yang patut diduga akan disalah gunakan oleh si-pelaku.
4. *Cyber Espionage (Spionase Cyber)*
   Suatu modus operandi kejahatan dunia maya yang memanfaatkan jaringan internet, untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara memasuki sistem jaringan komputer *(computer network system)* pihak yang menjadi sasarannya. Modus kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau data-data pentingnya (data base) tersimpan dalam suatu sistem yang *computerized* (terhubung dalam jaringan komputer).
5. *Cyber Sabotage and Extortion* (Sabotase dan Pemerasan Dunia Maya)
   Dalam kejahatan ini modus yang dilakukan biasanya dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga: data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya atau berjalan namun telah dikendalikan sesuai yang diinginkan oleh si pelaku.
6. *Offense Against Intellectual Property* (Pelanggaran Terhadap Hak atas Kekayaan Intelektual); Kejahatan ini modus operandinya ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai suatu contoh; peniruan tampilan pada suatu web page situs milik orang lain secara illegal. Penyiaran suatu informasi di internet yang ternya merupakan rahasia dagang orang lain dan sebagainya.
7. *Infringements of Privacy (Infringements privasi);* Modus pada kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized,* yang apabila diketahui oleh orang lain, maka dapat merugikan korban secara materiil maupun immaterial, seprti: bocornya nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan lain sebagainya.

Cyber Crime Simaks Online

Semakin canggihnya perkembangan komputer dan internet, membuat semakin berkembangnya dunia informasi yang berbasis teknologi ini. Sistem Informasi Managemen Akademik (SIMAK) Online adalah suatu sistem perencanaan yang merupakan bagian dari pengendalian internal suatu institusi pendidikan. Pemanfaatan yang dimaksud meliputi: manusia pada satu sisi, dokumen, teknologi dan Prosedur Operasional Standar (POS) pada

sisi yang lain, untuk dapat memecahkan berbagai permasalahan akademik. Permasalahan akademik tersebut meliputi: rencana studi, hasil studi, transkrip nilai, riwayat nilai, kartu hak ujian, daftar hadir mahasiswa, pengelolaan nilai, bimbingan akademik dan sebagainya. Sistem informasi manajemen akademik dibedakan dengan dengan sistem informasi pada umumnya karena SIMAK digunakan untuk menganaliasis sistem informasi yang diterapkan pada dunia pendidikan. Secara akademis, istilah ini umumnya digunakan untuk merujuk pada kelompok metode manajemen informasi yang bertalian dengan otoritas atau dukungan terhadap pengambilan keputusan manusia, sebagai suatu contoh: sistem pendukung keputusan, sistem pakar dan sistem informasi pimpinan. Sistem Informasi Manajemen Akademik adalah sebuah sistem yang lengkap, berguna untuk mendukung fungsi manajemen, akademik dan pengambilan keputusan dalam sebuah institusi pendidikan tinggi (http://www.fshuinsgd.ac.id/ lembaga-penunjang/simak/, download tgl 11 Juli 2016).

Sebagaimana kita ketahui bahwa dunia kampus merupakan dunia yang memiliki tingkat mobilitas yang cukup tinggi, apatah lagi kampus yang telah memiliki begitu banyak fakultas serta begitu banyak jurusan-jurusan dan program studi. Semakin banyak fakultas, jurusan dan program studi, mengakibatkan semakin banyak kegiatan-kegiatan akademis yang harus dilaksanakan dalam institusi pendidikan tinggi tersebut. oleh sebab itu, untuk dapat menujang kegiatan yang begitu banyak, SIMAK Online merupakan salah satu metode yang dapat digunakan untuk memberikan jalan keluarnya. Hal ini dapat penulis contohkan, Kinerja seorang dosen misalnya: sesuai dengan Undang-Undang No. 14 Tahun 2005 Tentang Guru dan Dosen serta dalam Peraturan Pemerintah No. 37 Tahun 2009 Tentang Dosen mengharuskan seorang dosen harus melaksanakan kinerja Tridarman Perguruan Tinggi yang meliputi: Pengajaran, Penelitian dan Pengabdian Kepada Masyarakat. Melihat begitu berat beban yang diamanatkan oleh Undang-Undang kepada seorang dosen, maka mengakibatkan seorang dosen harus bekerja dengan tanpa terbatas oleh "ruang dan waktu". Maksudnya adalah: dengan adanya Tridarma Perguruan Tinggi tersebut membebankan kepada seorang dosen harus beraktivitas "dimana-pun" dan "kapan-pun".

Kegiatan Penelitian dan Pengabdian misalnya: dalam melaksanakan kinerjanya seorang dosen harus melakukan kegiatannya tersebut dimana-pun dan kapan-pun , termasuk harus dilakukan jauh dari kampus dimana ia berasal. Sehingga dengan adanya hal tersebut mengakibatkan seorang dosen tidak dapat hanya berdiam diri dikampus dan/atau harus selalu berada dilingkunan kampus-nya. Tugas dosen adalah tugas yang "unik" , dan karena ke-unikannya itu lah Undang-Undang telah berusaha membuat alat ukur tersendiri terhadap kinerja dosen (*lex spesialis*) yang berbeda dengan cara mengukur kinerja pegawai pada umumnya. Dengan ada-nya Sistem Informasi Manajemen Akademik (SIMAK) yang dibuat secara ONLINE, memungkinkan dapat menunjang kegiatan seorang dosen yang "unik" tak terbatas ruang dan waktu tersebut. Seorang dosen dapat mengakses secara Online setiap kegiatan yang berkaitan dengan akademis-nya dimana-pun ia berada dan kapan-pun harus ia lakukan. Sebagai contoh: dalam mengentry penilaian bagi mahasiswa misanya, seorang dosen dapat mengakses dan mengentry penilaian tersebut kapan-pun dan dimana-pun ia berada sehingga kegiatan akademis penilaian tersebut tidak menjadi terhambat, oleh ruang

dan waktu. Begitupun juga bagi mahasiswa, dengan adanya SIMAK ONLINE ini mempermudah bagi mereka untuk mengetahui berbagai informasi yang menyangkut kegiatan akademis mereka tanpa harus dihambat oleh ruang dan waktu serta sistem birokrasi yang ada. Dengan Sistem Informasi Manajemen Akademik (SIMAK) membuat kegiatan dunia kampus (civitas akademika) lebih mudah dalam melakukan berbagai aktivitasnya terutama yang berkaitan dengan kegiatan akademis.

Perkembangan dunia cyber, mengakibatkan semakin canggihnya arus informasi berbasis komputer ini telah mengantarkan kita pada ruang-ruang yang seolah-olah tanpa sekat/dinding pemisah yang sering disebut dengan *"cyberspace"* (William Gibson, 1984: 151). *Cyberspace* seolah-olah menciptakan apa yang disebut dengan dunia tanpa batas *(borderless wolrd),* setiap orang siapa-pun dapat masuk dan bergabung ke dalamnya: siapa-pun dia, dimana-pun dia, kapan-pun dia. Keasikkan dalam *cyberspace* telah menciptakan dunia-nya tersendiri, dunia tanpa batas: baik batas kedaulatan negara, batasan-batasan etika bahkan batasan-batasan hukum sekalipun. Hal ini telah menimbulkan suatu kekhawatiran tersendiri bagi pengguna teknologi cyber ini, termasuk dikalangan perguruan tinggi. Penggunaan cyber adalah suatu "keniscayaan" yang tidak dapat dihindarkan, namun pada sisi yang lain kemungkinan terjadinya penyimpangan dalam dunia cyber selalu mengintai setiap saat. Termasuk juga kemungkinan terjadinya kejahatan dalam dunia cyber itu sendiri yang sering disebut dengan cyber crime terutama yang berkaitan dengan SIMAK ONLINE.

Berbicara mengenai cyber crime yang berkaitan dengan SIMAK online, tentunya menurut hemat penulis tidak dapat dilepaskan dengan modus-modus kejahatan yang sering terjadi dalam cyber space itu sendiri sebagaimana halnya terlah penulis kemukakan pada pembahasan terdahulu. Dalam beberapa literature yang ada, pengertian cybercrime sering diartikan sebagai *computer crime*. The US.Departement of Justice memberikan pengertian kejahatan komputer adalah:*"…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution".* Sedangkan menurut Andi Hamzah (1990) dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" memberikan arti bahwa *cyber crime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal. Melihat pengertian tersebut, maka cyber crime dapat dirumuskan sebagai suatu perbuatan melawan hukum yang dilakukan dengan memakai suatu jaringan komputer sebagai sarana dan/atau komputer sebagai objek untuk memperoleh keuntungan secara langsung atau-pun tidak dengan akibat merugikan pihak lain.

Berbicara mengenai SIMAK online tentunya tidak dapat dilepaskan dengan perangkat komputer atau teknologi yang menyerupainya (contoh: smart phone, tab, ipad dan sebagainya) serta jaringan internet yang selalui terkoneksitas antar satu dengan yang lainnya, sehingga memungkinkan terjadinya kegiatan elektronik melalui jaringan tersbut. SIMAK online sebagai suatu media yang merupakan salah satu fitur dalam E-Learning yang berkembang saat ini, memungkinkan bagi civitas akademika (komponen perguruan tinggi) secara cepat (online) untuk dapat mengakses berbagai kegiatan akademik. Oleh karena itu pemanfaatan SIMAK secara online dapat menjadi salah satu objek dalam *cyber crime* bagi pelaku-pelaku yang berpotensi untuk mengunakannya. Pelaku *cyber crime* yang berpotensi

menjadikan SIMAK online sebagai objek kejahatannya, tentu tidak dapat dilepaskan dengan kegiatan-kegiatan yang dilakukan dalam SIMAK itu sendiri, seperti penulis contohkan: masalah duplikasi, pemalsuan, pengrusakan, dan sebagainya. Melihat begitu luas pihak-pihak yang dapat berhubungan dengan SIMAK online tersebut, maka sudah barang tentu kemungkinan pelaku-pelaku kejahatannya-pun (penjahat) dapat dilakukan oleh "siapa-pun juga".

Sebagaimana halnya dalam ilmu kriminologi memberikan definisi "penjahat" adalah seseorang/sekumpulan orang yang melakukan suatu perbuatan jahat. Perbuatan jahat yang dimaksud dalam istilah kriminologi mengandung pengertian yang luas, karena tidak hanya meliputi perbuatan yang bertentangan dengan nilai-nilai sosial, agama juga meliputi aspek yuridis (hukum) itu sendiri. Oleh sebab itu, untuk mengkategorikan perbuatan jahat dalam *cyber crime* khususnya SIMAK Online, menurut hemat penulis harus dibatasi terlebih dahulu apa yang dimasksud dengan kegiatan jahatan dalam SIMAK online tersebut. Berdasarkan definisi kejahatan dalam kriminologi, penulis mencoba untuk memberikan batasan kejahatan yang dimaksud dalam SIMAK Online adalah: berbagai kegiatan/aktivitas yang dilakukan oleh seseorang atau sekumpulan orang-orang yang dapat menimbulkan kerugian baik secara langsung atau tidak langsung yang berhubungan dengan SIMAK Online.

Demikian-pun dalam menentukan siapa "penjahat" yang dimaksud dalam *cyber crime* SIMAK Online, juga harus ditentukan terlebih dahulu siapa penjahat tersebut. Dalam hal ini yang dimaksud dengan penjahat adalah: seseorang/sekumpulan orang-orang yang karena tindakannya dapat menimbulkan kerugian baik secara langsung/tindak langsung yang berkaitan dengan SIMAK Online. Apabila melihat modus yang dilakukan dalam *cyber crime* SIMAK Online ini, maka pelaku yang berpotensi melakukan kejahatan tersebut adalah orang-orang atau sekumpulan orang-orang yang tentunya memiliki hubungan baik secara langsung atau-pun tidak langsung dengan kegiatan/aktivitas SIMAK Online itu sendiri. Sebagaimana halnya dalam hukum pidana yang mengatur mengenai tindak pidana *(strafbaarfeit)*, berusaha memberikan ukuran-ukuran yang pasti/jelas apa yang dimaksud tindak pidana tersebut.

Dengan adanya ukuran-ukuran tersebut, maka dapat dibedakan antara perbuatan pada umumnya dengan perbuatan yang terkategori dengan tindak pidana. Dalam hukum pidana ukuran-ukuran yang dimaksud tersebut dituangkan dalam unsur-unsur tindak pidana. Unsur-unsur tindak pidana memberikan batasan-batasan yang jelas/pasti tentang apa-apa saja yang menjadikan perbuatan tersebut terkategori tindak pidana. Antara unsur yang satu dan unsur yang lain saling berkaitan serta berusaha memberikan penjelasan bagi yang lainnya.

Dengan demikian dapat disimpulkan bahwa *cyber crime* dalam SIMAK Online: adalah berbagai macam kegiatan atau aktivitas yang dilakukan oleh seseorang atau sekumpulan orang-orang yang patut diduga (pegawai, mahasiswa, ataupun dosen itu sendiri) berpotensi untuk melakukan kegitan/aktivitas yang dapat menimbulkan kerugian baik secara langsung atau-pun tidak langsung yang berkaitan dengan SIMAK Online. Tindakan sebagaimana dimaksud tentunya adalah kegiatan yang illegal (tidak berizin/resmi) yang memiliki tujuan-tujuan tertentu yang dapat

menimbulkan terganggunya kegiatan belajar-mengajar, khususnya diperguruan tinggi dimana SIMAK Online itu diterapkan/digunakan.

Penegakan Hukum dan Upaya Pencegahan *Cyber Crime* SIMAK Online

Berbicara mengenai penegakan hukum terutama masalah *Cyber Crime* dalam SIMAK Online, tentunya tidak dapat dilepaskan dengan kegiatan penegakan hukum *Cyber Crime* di Indonesia secara keseluruhan. Sementara pada sisi lain berbicara masalah penegakan hukum Cyber Crime-pun juga tidak dapat dilepaskan dengan masalah penegakan hukum pidana secara keseluruhan. Berbicara masalah penegakan hukum pidana secara keseluruhan sangatlah dipengaruhi oleh berbagai aspek dalam bekerjanya hukum pidana itu snediri. Hal ini sebagaimana yang dikemukakan oleh Lawrence M. Friedman yang dikutip oleh Kadri Husin (1999: 7), menunjukkan tiga aspek di dalam bekerjanya sistem hukum, yaitu;

a. *aspek struktural* yaitu: aparat penegak hukum dalam melaksanakan penegakan hukum dibatasi tingkat kemampuan atau profesionalitas maupun terbatasnya biaya, sumber daya manusia, sarana dan prasarana.
b. *aspek kultural/budaya* yaitu: aspek yang muncul pada diri aparat penegak hukum yang disebabkan adanya pengaruh dari aspek nilai dan sikap, baik dari dalam organisasi fungsionaris hukum sendiri ataupun pengaruh dari lingkungan sekitarnya*;*
c. *aspek substantif* yaitu: aspek yang disebabkan adanya kelemahan dalam undang-undang yang ada baik dari segi materiil maupun formil*.*

Berkerjanya sistem hukum dalam masyarakat untuk menyelesaikan persoalan kejahatan sangat dipengaruhi ketiga aspek tersebut di atas. Dengan meminimalisir kemungkinan timbulnya berbagai kelemahan yang terdapat diketiga aspek tersebut, memungkinkan penegakkan hukum pidana dalam menyelesaikan persoalan kejahatan di dalam masyarakat dapat maksimal. Sebagaimana halnya dalam penegakan hukum pidana *Cyber Crime*-pun sangat dipengaruhi oleh adanya ketiga aspek tersebut di atas. Hal ini sebagaimana penulis kemukakan bahwa *cyber crime* merupakan kejahatan dengan dimensi *"high-tech"* sehingga memerlukan cara-cara penegak hukum yang benar-benar professional: dalam pengertian bahwa sepenuhnya memahami masalah tersebut. Selain itu, dalam penegakan hukum *cyber crime* memerlukan dana/anggaran yang cukup besar terutama untuk mengirim aparat penegak hukum untuk diberikan pelatihan Sumber Daya Manusia baik di dalam negeri maupun diluar negeri.

Ketiadaan laboratorium forensik komputer di Indonesia menyebabkan penyelidikan dan penyidikan *cyber crime* menjadi lamban karena proses forensik tersebut harus dilakukan diluar negeri. Belum lagi citra lembaga peradilan yang belum membaik, meskipun berbagai upaya telah dilakukan sehingga menyebabkan banyak orang yang menjadi korban dalam *cyber crime* enggan untuk melaporkan kasusnya ke Kepolisian. Dengan demikian menyebabkan *dark number* (angka gelap) dalam penanganan kasus *cyber crime* semakin meningkat. Upaya penanganan *cyber crime* membutuhkan keseriusan dari berbagai pihak mengingat perkembangan teknologi informasi khususnya internet sudah menjadi sesuatu keharusan dalam rangka untuk membangun masyarakat yang berbudaya informasi.

Mengingat begitu banyak faktor-faktor yang menjadi penghambat dalam penegakan hukum pidana *cyber crime*, maka sudah seharusnya

pemerintah pada satu sisi dan fungsionaris hukum pada sisi yang lain termasuk juga komponen masyarakat khusunya perguruan tinggi di dalamnya untuk mencari solusi dalam rangka menyelesaikan berbagai kelemahan tersebut. Dengan mengatasi berbagai problem kelemahan tersebut, paling tidak satu langkah kedepan solusi penyelesaian dalam penegakan hukum pidana dalam *cyber crime* dapat sesuai dengan apa yang di harapkan. Mengidentifikasi persoalan dalam penegakan hukum pidana *cyber crime* menurut hemat penulis dapat dimulai secara *intern* (dalam sistem peradilan pidana) maupun secara *ekstern* di luar sistem tersebut.

Secara intern dapat dicontohkan: meminalisir kemungkinan timbul berbagai persoalan dalam sistem peradilan pidana sendiri baik secara formiil maupun secara materiil. Secara formil miasalnya dalam proses penyelidikan-penyidikan-penuntutan: adanya berbagai keterbatasan kemampuan yang dimiliki oleh aparat penegak hukum dalam memahami persoalan pengungkapan suatu kasus dalam *cyber crime* yang nota bene berkaitan langsung dengan penggunaan ilmu pengetahuan dan teknologi yang canggih (teknologi internet dan komputer), serta pelaku-pelaku nya yang memiliki keahlian khusus yang tidak dimiliki oleh orang-orang pada umumnya termasuk keahlian untuk menghindar dari jeratan hukum yang ada.

Keterbatasan sarana-prasarana yang dimiliki penegak hukum dalam rangka pengungkapan kasus *cyber crime* harus segera dituntaskan, hal ini menjadi sesuatu yang sangat mendesak mengingat perkembangan dunia *cyber crime* begitu cepat baik kualitas maupun kuantitasnya. Belum lagi berbicara mengenai pembuktian tentang diduganya suatu kejahatan dunia maya/internet yang memerlukan sistem pembuktian yang tidak sesederhana sebagaimana hal nya dalam pembuktian dalam tindak pidana pada umumnya. Oleh sebab itu, menurut hemat penulis upaya sedini mungkin yang dapat dilakukan dalam rangka penegakan hukum pidana *cyber crime* adalah: menyelesaikan berbagai persoalan-persoalan keterbatasan tersebut di atas, tidak hanya dihilir juga dari hulu-nya.

Secara materiil adalah dengan menerapkan ketentuan-ketentuan pidana secara konsisten baik yang diatur secara umum maupun ketentuan-ketentaun yang diatur secara khusus. Ketentuan secara umum yang dimaksud adalah dengan diterapkannya ketentuan pasal-pasal yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) kepada pelaku *cyber crime* seperti sebagai berikut: Pasal 362 KUHP dikenakan untuk kasus Carding dimana pelakunya telah melakukan pencurian nomor kartu kredit milik orang lain meskipun tidak secara fisik, karena yang diambil hanya nomor kartunya saja. Pasal 378 KUHP dapat diterapkan untuk pelaku penipuan. Pasal 335, 311, 303, 282, 281, 378, 262, 406, 112,113,114, 115 dan 116 KUHP. Selain diterapkannya berbagai Pasal-pasal dalam KUHP ketentuan yang bersifat khusus-pun *(spesialis)* dimungkinkan untuk diterapkan seperti: Undang-Undang No.19 Tahun 2002 Tentang Hak Cipta, Undang-Undang No.36 Tahun 1999 Tentang Telekomunikasi, Undang-Undang No.8 Tahun 1997 Tentang Dokumen Perusahaan, Undang-Undang No.25 Tahun Tahun 2003 Tentang Perubahan atas Undang-Undang No.15 Tahun 2001 Tentang Tindak Pidana Pencucian Uang. Undang-Undang No.15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Undang-Undang No.11 Tahun 2008 Tentang Internet dan Transaksi Elektronik.

Kesimpulan

Sebagai salah satu upaya yang rasional dalam mengatasi kejahatan dalam masyarakat termasuk *cyber crime*, sarana penal (hukum pidana) nampaknya merupakan suatu cara yang dapat digunakan dengan menerapkan sanksi pidana kepada pelaku tindak pidana yang terkategori dalam *cyber crime.* Namun mengingat berbagai dampak negatif dalam penerapan sarana' penal (hukum pidana) kepada pelaku tindak pidana dan mengingat berbagai keterbatasan serta berbagai aspek-aspek yang memungkinkan bekerjanya hukum pidana dalam menanggulangi cyber crime dalam masyarakat, maka hendaknya penggunaan *upaya penal (hukum pidana)* tetap di damping dengan *upaya non-penal* (diluar hukum pidana).

Upaya non-penal merupakan *upaya ekstern* (diluar hukum pidana) yang dapat dilakukan dalam rangka untuk mendukung upaya penal dalam menyelesaikan persoalan *cryber crime,* upaya ini dapat penulis contohkan; memperketat berbagai sistem keamanan *(safety)* dalam berbagai kegiatan akses-akses penting yang menggunakan media internet dan komputer, terlebih khusus diperguruan tinggi yang menggunakan SIMAK online. Dengan upaya ini, seolah-olah terdapat benteng berlapis yang memberikan perlindungan bagi pengguna internet sehingga mempersulit pelaku *cyber crime* untuk menembus/mengakses secara illegal situs/web tersebut. Upaya non-penal lainnya dapat penulis contohkan adalah: dengan memberikan penyuluhan baik secara formal maupun non-formal kepada masyarakat pengguna internet terlebih khusus masyarakat kampus, tentang pemahaman yang benar, bahwa teknologi internet hendaknya dipergunakan secara bijaksana dan bertanggung jawab, sehingga kemajuan teknologi internet tersebut dapat memberikan manfaat bagi si-penggunanya bukan sebaliknya.

Dengan adanya keterpaduan sarana penal dan non-penal serta meminimalisir kemungkinan timbulnya berbagai kelemahan dalam mengatasi persoalan *cyber crime* khususnya dalam SIMAK online, maka apa yang diharapkan dapat benar-benar terwujud. Namun pertanyaan lebih lanjut adalah, apakah semua persoalan yang berkaitan dengan *cyber crime* secara umum dan persoalan SIMAK online secara khsus dapat diselesaikan? maka untuk dapat menjawab pertanyaan tersebut akan kembali kepada diri "kita" sendiri (pengguna internet), baik kita sebagai pribadi (personen) maupun kita sebagai keseluruhan (jamak).

Daftar Pustaka

Abdul Wahid dan Muhammad Habib. *Kejahatan Mayantara (Cyber Crime).* (Bandung: Refika Aditama, 2005)

Agus Raharjo. *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Citra Aditya Bakti, Bandung, 2002.)

Amirudin dan Zainal Askin. *Pengantar Metode Penelitian Hukum*, (Jakarta: Raja Grafindo Persada, 2004)

Andi Hamzah. *Kamus Hukum*, (Ghalia Indonesia, Jakarta, 1986)

--------.*Aspek-aspek Pidana di Bidang Komputer*, (Jakarta: Ghalia, 1989)

--------.*Pengenalan Komputer (Introduction to Computer).* (Institut Komputer Indonesia (IKI), 2001)

Barda Nawawi Arief. *Masalah Penergakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulanggan Kejahatan,* (Jakarta: Kencana Predana Media Group, 2007)

Budi Raharjo. *Memahami Teknologi Informasi,* (Jakarta: Elexmedia Komputindo, 2002)

Casey, Eoghan. *Digital Evidence and Komputer Crime*, (London: A Harcourt Science and Technology Company, 2001)

Kadri Husin. *Diskresi Dalam Penegakan Hukum Pidana Di Indonesia (Suatu Analisis Penegakan HAM Dalam Peradilan Pidana),* (Pidato Pengukuhan Guru Besar Ilmu Hukum Universitas Lampung, 1999)

William Gibson, *Neuromancer*, (New York: Ace. 1984)

Internet:

Dimitri Mayahana, "Tingkat Cyber Crime di Indonesia Mengkhawatirkan", http://nationalgeographic.co.id/berita/2014/10/ (Download Tgl 10 November 2015 Pkl 21.00 wib)

HerryHeryawan, *Bos Penipuan SMS Mama Minta Pulsa Ditangkap* http://news.liputan6.com/read/2358365/ (Download Tgl 7 November 2015 Pukul 21.00 wib)

Iqbal, *Jumlah kasus kejahatan di dunia maya (cyber crime) di Jakarta yang ditangani Kepolisian Daerah Metro Jakarta Raya meningkat*. https://m.tempo.co/read/news/2015/09/21/064702312/(Download, tgl 6 Nov 2015 Pukul 20 wib)

Irwan, *"Pengaduan tiga bank, yang satu 47 nasabah, satunya sekitar 30 nasabah kemudian ketiga 27 nasabah,"* http://bisnis.liputan6.com/ read/2214402/hacker-bobol-ratusan-rekening-nasabah-bank (Download tgl 5 Nov 2015 Pukul 17 wib)

Krishna, *64 WN Taiwan Penipu Online Lintas Negara Dideportasi* http://www.liputan6.com/tag/penipuan-online (Download tgl 7 Nov 2015 pukul 22.30 wib)

Simak fakultas syariah uin sunan gunung jatih, http://www.fshuinsgd.ac.id/lembaga-penunjang/simak/ (Download tgl 11 Juli 2016, Pukul 24.30 wib)

Undang-Undang:

Kitab Undang-Undang Hukum Pidana;

Undang-Undang No.8 Tahun 1997 Tentang Dokumen Perusahaan;

Undang-Undang No. 36 Tahun 1999 Tentang Telekomunikasi;

Undang-Undang No.19 Tahun 2002 Tentang Hak Cipta;

Undang-Undang No.15 Tahun 2011 Tentang Perubahan atas Pencucian Uang;

Undang-Undang No.15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme;

Undang-Undang No,11 Tahun 2008 Tentang Internet dan Transaksi Elektronik.